UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/035,464	12/31/2001	Ron W. Rogers	9973	4003

26884 7590 04/21/2006

PAUL W. MARTIN
NCR CORPORATION, LAW DEPT.
1700 S. PATTERSON BLVD.
DAYTON, OH 45479-0001

EXAMINER	
HEWITT II, CALVIN L	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 04/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/035,464
Filing Date: December 31, 2001
Appellant(s): ROGERS ET AL.

James D. Wood, Reg. No 43,285
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 09 January 2006 appealing from the Office action mailed 11 May 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,502,135	MUNGER et al.	12-2002
WO 00/46959	NORDENSTAM et al.	10-2000
4,262,359	CORY et al.	4-1981

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nordenstam et al., International Publication Number WO200046959 in view of Cory et al., U.S. Patent No. 4,262,359 and Munger et al. U.S. Patent No. 6,502,135.

As per claims 1-20, Nordenstam et al. teach a system for transmitting data from a wireless terminal to a host computer in a store (figure 3; page/line 19/4-20/8; page 21, lines 5-25). Nordenstam et al. also teach transmitting encrypted information from said wireless terminal (page 25, lines 15-20). Regarding "load balancing", it is well known to those of ordinary skill in networking to monitor network traffic and perform "load balancing" to prevent the overloading of circuits at a receiving node or station. Therefore, it would have been obvious in light of the teachings of Nordenstam et al. to utilize load balancing in order to reduce the load on a transaction terminal (page 19, lines 4-15). Nordenstam et al. do not explicitly recite transmitting "bogus messages". Cory et al. disclose a secure method and system for transmitting data over a network by coupling a "bogus message" generator to a transmission source (column 1, lines 24-28) and

inserting encrypted "bogus messages" during the "dead space" (i.e. dead space greater than a threshold or "non-zero" or the existence of dead space) between valid messages (column 1, lines 13-27), which are in turn, decrypted and filtered out upon reception by a receiver (column 1, lines 19-24 and 28-34). Hence, Cory et al. teach transmitting bogus messages in response to an actual message. However, neither Nordenstam et al. nor Cory et al. teach monitoring a parameter on the receiving end of a transmission and using said parameter to trigger the generation and transmission of a bogus message. Munger et al. teach a method for generating "bogus messages" at a transmission node based on monitored network traffic conditions (column 10, lines 15-34; column 12, lines 20-30).For example, Munger et al. teach generating bogus messages randomly or based on time of day and during low traffic (column 12, lines 27-33). The Munger et al. system, however, is not limited to any particular algorithm (column 12, lines 26-28). The only requirements of the Munger et al. teaching is that the chosen algorithm generate bogus messages for foiling malicious traffic analysis efforts (column 12, lines 20-26). Hence, it would have been obvious to one of ordinary skill, in light of the clear teachings of Munger et al., to utilize any algorithm as long as it is in accordance with the policies and desires of the network managers for creating a secure network. Therefore, it would have been obvious to one of ordinary skill to combine the teachings of Nordenstam et al., Cory et al. and Munger et al. in order to protect sensitive data, such as credit card data,

transmitted over the network of Nordenstam et al. ('959, figure 3) from malicious traffic analysts ('359, column 1, lines 12-18; '135, column 10, lines 12-21).

(10) Response to Argument

Restrictions are not subject to appeal so the Examiner has not responded to Appellants arguments directed to the validity of the Restriction (Office Action dated, 11 May 2005).

The Examiner withdraws the 101 and 112 Rejections.

Claims 1-3, 6, 7, 15-17

Appellant is of the opinion that the prior art of Nordenstam et al., Cory et al. and Munger et al. is not combineable. Specifically, Appellant asserts that because Nordenstam et al. teach communicating via Bluetooth and Cory et al. teach continuous transmission, any combination of the two systems would result in a "breaking" of Nordenstam et al. (Appeal Brief, p19, third full paragraph, lines 1-6). However, this analysis of Cory et al. is inaccurate, and derives only from a gross, and intentional, misreading of the Cory et al. patent. For example, Appellant states that the "Examiner misidentified the teachings of Cory et al. (Appeal Brief, p19, first full paragraph, lines 1-

2). This attempt at misdirection is an effort to draw the Board's attention away from Cory et al. disclosure of the state of the art at the time of their invention. Cory et al. state

> In transmitting teletype messages that may be received by the enemy it has been customary to feed the teletype tape through a transmitter having cryptographic equipment. To secure traffic flow security it is desirable to insert dummy messages in the breaks between the valid messages ('359, column 1, lines 13-18).

Teletype communication is discrete. Therefore, one of ordinary skill would know to transmit messages at discrete intervals, note the background of the invention of Cory et al. do not require continuous transmission of dummy messages only to insert these messages in between "real ones" ('359, column 1, lines 13-18). Hence, Nordenstam et al. teaches a wireless terminal in connection to a master terminal (WO'959, figure 3, item 22; page/line 19/4-20/8; page 21, lines 5-25), while Cory et al. disclose a bogus message transmitter connected to a sending terminal ('359, column 1, lines 13-18), in this case the wireless terminals of Nordenstam et al. (WO'959 figures 3 and 12), for sending generating bogus messages in order to confound malicious entities who desire to steal information (359, column 1, lines 13-18) transmitted to the host or master terminal such as credit card numbers (WO'959, page 21, lines 5-25).

Regarding "a communication parameter regulator for measuring a communication parameter on the store host computer, the communication parameter regulator operable to activate in accordance with the measured communication parameter", Munger et al. teach a terminal transmitting bogus messages according to

an algorithm, such as traffic ('135, column 12, lines 30-35). In Munger et al., traffic is determined by the terminal or router. However, in the context of Nordenstam et al. traffic is monitored by the master or host terminal (WO'959, figure 3, item 22), hence in Nordenstam et al. the host terminal would transmit a signal to the mobile devices to start generating bogus messages. The question then remains is this analysis supported by the prior art of Nordenstam et al.?

Appellant correctly notes that in Nordenstam et al., messages are exchanged between wireless terminal and master terminal using the Bluetooth protocol (Appeal Brief, page 15, last full paragraph, lines 1-2). In Bluetooth, communication is controlled by, for example, a master device (i.e. master terminal) (Appeal Brief, page 16, second full paragraph, lines 4-5). More specifically, Appellant states "The master device also controls access to the physical data communications channel" and "... slave terminals are only allowed to transmit data to the master device of the piconet during certain restricted timeframes" (Appeal Brief, page 16, last full paragraph- page 17, lines 1-2) and that "slave terminals are only allowed to transmit data to the master terminal *at specified times established by the master terminal*" (emphasis added) (Appeal Brief, page 17, first full paragraph, lines 5-7). The teaching of Nordenstam et al. supports Appellant's assessment as Nordenstam et al. identifies the master terminal as the regulator of traffic (i.e. load) on the Bluetooth LAN (WO'959 abstract; page 13, lines 1-32; page 14, lines 1-3 and 15-18; page 15, lines 11-17; page/line 19/4-20/8; page 21, lines 5-25; page 22, lines 5-10). Hence, in order to generate a bogus message in

Nordenstam et al., the master terminal (WO'959 figure 3, item 22) would transmit to the wireless terminal, based on data measured stored at the master (i.e. the data used by the master to regulate traffic such as the data used to establish times for receiving data from the slave terminal- WO'959, page 14, lines 1-3 and 15-18), a signal indicating that the wireless terminal can send bogus messages ('359, column 1, lines 13-18). Further, this data measured at the master is traffic (i.e. load) data (WO'959 page 14, lines 1-3 and 15-18; page/line 19/4-20/8; page 21, lines 5-25) and according to Munger et al. would be used by the wireless terminal to initiate the generation of bogus messages ('135, column 12, lines 25-33). Therefore, the contrary to the Appellant's contention Nordenstam et al., Cory et al. and Munger et al. are combineable and the reasons for such a combination are set forth by Cory et al.:

> To secure traffic flow security it is desirable to insert dummy messages in the breaks between the valid messages ('359, column 1, lines 13-18).

Note the claim does not specify the location of the "parameter" regulator, hence a reasonable interpretation of claim 1 would locate it at the host terminal (see also Appellant's Spec. paragraph 19).

As an aside, Nordenstam et al. discloses a wireless terminal selecting a LAN (WO'959, page 19, lines 17-29). However, since the Bluetooth LAN is in existence the master terminal (e.g. figure 3) has already been established.

Claims 4, 13 and 20

Regarding claim 4, Appellant is of the opinion that the prior art does not teach terminating bogus message generation "in response to a bona fide transaction occurring" at the terminal. The Examiner respectfully disagrees as Munger et al. disclose generating dummy packets when the system is idle ('135, column 12, lines 26-30). Hence, a fair reading of the prior art implies that in order for this to happen there would not be any bogus messages generation when the system is not idle. Further, Appellant's analysis ignores the clear teachings of Cory et al. and Munger et al. which detail generating bogus messages when there are no valid messages ('359, column 1, lines 16-18; '135, column 12, lines 26-30).

Claim 5

Appellant is of the opinion that the prior art does not disclose a "load balancer that generates a bogus message request". The Examiner respectfully disagrees. Initially, the Examiner would like to point out that although the claims are to be interpreted in light of the Specification, limitations from the Specification are not to be read into the claims (*In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993)). The Examiner maintains the assertion that load balancing is old and well known (Final Office Action, dated 11 May 2005). The Examiner also maintains his assertion (Final Office Action, dated 11 May 2005, "Response to Arguments") that a load balancer in the context of Nordenstam et al. would be located at the host or master terminal

(WO'959 figure 3, item 22; page 14, lines 1-3 and 15-18; page/line 19/4-20/8; page 21, lines 5-25), a conclusion, recognized by the Appellant (Appeal Brief, page 15, last full paragraph, lines 1-2; page 16, second full paragraph, lines 4-5; page 16, last full paragraph- page 17, lines 1-2 and 5-7), and supported by the use of Bluetooth technology in the Nordenstam et al. teaching (WO'959 page 14, lines 1-3 and 15-18). According to the claim, Appellant's load balancer "generates a bogus message request in response to the computed dead space being greater than a threshold". Therefore, since the combined prior art performs the function of generating a bogus message request in response to the computed dead space being greater than a threshold, the device or devices that perform said function reads on a "load balancer". Recall, in a Bluetooth environment, the slave terminals, in this case the wireless terminal (WO'959, figure 3, items 10A-C), sends messages according to the instructions of the master terminal (WO'959, figure 3, item 22), while Cory et al. and Munger et al. explicitly teach generating bogus messages when the system is idle, or equivalently, in between valid messages ('359, column 1, lines 16-18; '135, column 12, lines 26-30). As correctly characterized by the Appellant (Appeal Brief, page 15, last full paragraph, lines 1-2; page 16, second full paragraph, lines 4-5; page 16, last full paragraph- page 17, lines 1-2 and 5-7), the host terminal (figure 3, item 22) in Nordenstam et al. is responsible for informing the wireless terminal when to send data. Munger et al. teach generating dummy packets when the system is idle ('135, column 12, lines 26-30). Again according

to Appellant, system traffic in the Nordenstam et al. system is monitored at the master terminal. Hence, when the "idle" time, or time in between valid messages is greater than zero (i.e. greater than a threshold, where zero is the threshold), the master sends a message to the terminal to generate and send a bogus message.

Cory et al. recite in order to secure traffic flow it is desirable to insert dummy messages in the breaks between valid messages ('359, column 1, lines 15-18). In the Nordenstam et al. system, there are many terminals communicating with a single master on a Bluetooth LAN (WO'959 abstract; figures 3 and 12; page 13, lines 1-32; page 14, lines 1-3 and 15-18; page 15, lines 11-17; page 22, lines 5-10), hence breaks in the system (i.e. the network of wireless terminals and host terminal) can only be determined by the master terminal, therefore, the combined prior art teaches generating a bogus message request in response to the computed dead space (by the master terminal-WO'959 abstract; figures 3 and 12; page 13, lines 1-32; page 14, lines 1-3 and 15-18; page 15, lines 11-17; page 22, lines 5-10), being greater than a threshold ('359, column 1, lines 16-18; '135, column 12, lines 26-30).

Claims 8-12 and 14

Appellant's analysis of the prior art is piecemeal as Appellant considers only what is or isn't taught by Cory et al. regarding "load". However, it has been held that one cannot argue nonobviousness by considering references individually when the rejection

is based on a combination of the references (*In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986)). The Examiner did not rely on Cory et al. to teach load. On the other hand, Nordenstam et al. discloses a host computer in communication with a plurality of wireless terminals is a retail environment (WO'959 page 19, lines 4-15). Specifically, Nordenstam et al. teaches a plurality of wireless terminals in communication with store terminals (WO'959 abstract; figure 3) over a Bluetooth LAN wherein one of the terminals serves as a master terminal (WO'959 page 14, lines 1-3 and 15-18; page 15, lines 11-17) for regulating traffic (i.e. load) on the network (WO'959 page 14, lines 1-3 and 15-18). Cory et al. teach generating bogus messages in between valid messages ('359, column 1, lines 11-17), while Munger et al. explicitly teach generating messages based on low traffic ('135, column 12, lines 30-33). In Nordenstam et al., traffic is determined at the master terminal and not at the wireless or slave terminals, as the master terminal regulates traffic on the Bluetooth LAN (WO'959 page 14, lines 1-3 and 15-18). Hence, the combined prior art teaches Appellant's claims 8-12 and 14.

Claims 18 and 19

Appellant is of the opinion that the prior art does not teach "generating bogus messages until a bogus message timer expires." The Examiner respectfully disagrees.

Munger et al. explicitly recite generating bogus messages based on time of day ('135, column 12, lines 30-33). Time of day is measured by clock, hence Munger et al. teach a timer. Further, there is necessarily a time when the bogus generator of Munger et al. stops generating bogus messages otherwise, the messages would be generated around the clock and there would be need for an initiation of bogus message creation based on a time of day.

Conclusion

The rejection should be sustained because the Appellant's analysis only considers what Nordenstam et al., Cory et al. and Munger et al. teach individually and not what the prior art teaches in combination. Appellant also fails to consider the combination in light of Bluetooth technology and the broad teachings of Munger et al. regarding algorithms for generating bogus messages.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Calvin Loyd Hewitt II

(Conferee)

Conferees:

James P. Trammell

Hyung Sough